ANDROID THINGS

Mg. Ing. Norma Beatriz Perez[(1)], Miguel Alfredo Bustos[(1)], Dr. Mario Marcelo Berón[(1)] & PhD. Pedro Rangel Henriques[(2)]
[(1)]Departamento de Informática – Facultad de Ciencias Físico Matemáticas y Naturales (FCFMyN) – Universidad Nacional de San Luis (UNSL)
Ejercito de los Andes 950, D5700HHW San Luis, +54-0266 4520300 – Int. 2103
[(2)] Departamento de Informática – Universidade do Minho – Braga, Portugal
{*mabustos, nbperez, mberon*}*@unsl.edu.ar - pedrorangelhenriques@gmail.com*

RESUMEN

En la actualidad, el *Internet of Things* (IoT) supera a los smartphones convirtiéndose en la categoría más importante de dispositivos conectados. Este ingente crecimiento de IoT impulsa a los desarrolladores de estas tecnologías evolucionar en el enfoque de la seguridad para proteger servicios vitales, información sensible de posibles robos, manipulación y pérdida de datos además de otros aspectos claves que permitan diseñar sistemas IoT confiables. Es por esto, que las organizaciones de desarrollo como Google, Apple se introducen en este mercado global incorporando a su staff plataformas emergentes de IoT. *Android Things* es una plataforma de vanguardia que provee Google para el desarrollo de dispositivos versátiles, de bajo costo, de calidad, entre otras características de relevancia que simplifican y satisfacen las necesidades de los usuarios que son cada vez más exigentes.

El presente trabajo describe una línea de investigación que estudia de manera exhaustiva la plataforma Android *Things* pensada principalmente para la implementación de objetos integrados e interconectados. Dicho estudio se fundamenta en la utilización de la plataforma Android *Mobile* como soporte para construir aplicaciones de Android *Things* confiable*s*. El análisis de estas tecnologías se basa detectar los principales lineamientos para proponer y desarrollar un metodología o herramienta que permita migrar aplicaciones existentes al nuevo mercado de Android *Things* de manera segura.

Palabras Claves: Android, Android *Things*, Aplicaciones, Seguridad.

CONTEXTO

La presente línea de investigación se enmarca en dos Proyectos de Investigación. El primero: "*Ingeniería de Software: Conceptos, Prácticas y Herramientas para el Desarrollo de Software con Calidad*" – Facultad de Ciencias Físico Matemáticas y Naturales de la Universidad Nacional de San Luis. Proyecto Nº P-031516 que es la continuación de diferentes proyectos de investigación, a través de los cuáles se ha logrado un importante vínculo con distintas universidades a nivel nacional e internacional. Además, se encuentra reconocido por el Programa de Incentivos. El segúndo proyecto: "*Fortalecimiento de la Seguridad de los Sistemas de Software mediante el uso de Métodos, Técnicas y Herramientas de Ingeniería Reversa*" realizado en conjunto con la Universidade do Minho Braga, Portugal, fue aprobado por el Ministerio de Ciencia, Tecnología e Innovación Productiva (MinCyT), y su código es PO/16/93.

1. INTRODUCCÓN

La aceptación global de la Internet; la gran dispersión de usuarios móviles; los miles de millones de dispositivos que se conectan entre sí con el auge de IoT; así como la enorme acumulación de información en la nube hacen que su uso e incorporación en los diferentes escenarios sea un reto primordial en los mercados emergentes donde se emplean estas tecnologías. El lanzamiento de la plataforma Android [1], [2] ha causado gran

impacto en el desarrollo de aplicaciones móviles [3] logrando una amplia aceptación en el mercado global donde cada vez las partes involucradas son más exigentes.

Hoy en día, la plataforma Android [4] se ha convertido en una alternativa dominante frente a otras plataformas. Esta plataforma se basa en el sistema operativo Linux por lo que es de código abierto y puede ser utilizado sin realizar costos adicionales a sus usuarios. Se destaca por ser adaptable a cualquier tipo de hardware como por ejemplo, Smartphone, Smartwatch, etc. y una amplia variedad de productos empotrados que utilizan este sistema operativo para llevar a cabo sus tareas. Las aplicaciones, en la plataforma Android, son desarrolladas en el lenguaje JAVA [5] esto permite que dichas aplicaciones pueden ser ejecutadas en cualquier dispositivo a través de la máquina virtual denominada Dalvik [6] ofreciendo portabilidad segura. Por otro lado, la arquitectura de Android [7] se basa en componentes "inspirados" en Internet. Por ejemplo, la interfaz de usuario es realizada en XML permitiendo que una misma aplicación se ejecute en diferentes pantallas bajo distintas dimensiones. Android incorpora servicios de localización [8], acceso a redes, bases de datos con SQL, síntesis de voz, multimedia, entre otros. La seguridad de Android [9] se provee a través de permisos que son otorgados por parte de sus usuarios.

La plataforma Android *Mobile* ofrece una manera intuitiva y novedosa de desarrollar e implementar potentes aplicaciones para diversos dispositivos. Android *Things* [10] extiende de la plataforma Android *Mobile* con el objetivo de ofrecer a los desarrolladores la posibilidad de construir objetos integrados e interconectados con características destacables como es la alta calidad, mayor seguridad, productos a escala, etc. Se destacan tres pilares primordiales de esta plataforma con respecto a Android *Mobile*: Arquitectura (incorporando una extensión del marco central con APIs adicionales que ofrece la biblioteca de soporte *Things*); Actualizaciones seguras (son administradas por la central de Google); Optimización de Sistema Operativo [11] (se dispone de una variante con el objetivo de ser utilizado en IoT [12]) y Hardware potente (accesible y de fácil integración). Es por esto, que la línea de investigación aborda el estudio de los pilares mencionados previamente.

2. LÍNEAS DE INVESTIGACIÓN Y DESARROLLO

En la actualidad, para la implementación y desarrollo de aplicaciones IoT que utilizan como soporte la plataforma Android *Things* es una tarea intuitiva si el desarrollador a programado previamente bajo Android. Esto se debe a que la migración de aplicaciones desarrolladas en Android *Mobile* (que utilizan el entorno de desarrollo integrado Android Studio [13], [14], APIs, etc.) a Android Things resultan en una convergencia relativamente simple debido a que ambas plataformas comparten características similares por ser implementadas por la misma organización de desarrollo denominada Google. La popularidad de Android se debe a la amplia aceptación de sus usuarios en este mercado.

IoT está en pleno auge incorporando aplicaciones móviles que facilitan el uso, administración y control de los dispositivos que intervienen en un sistema IoT. Sin embargo, IoT trae asociado riesgos de seguridad, presentando en ocasiones fallas de carácter crítico pudiendo vulnerar a organizaciones, gobiernos, usuarios potenciales, entre otros.

Por otro lado, Android *Things* es una tecnología emergente que incorpora actualizaciones seguras con el objetivo de evitar perdida de información relevante, contrarrestar las amenazas, etc.

Lo mencionado en los párrafos anteriores, deja en evidencia que los desarrolladores de aplicaciones basado en

Android *Things* se enfrentan a un problema principal que es la creación de actualizaciones seguras y escalables ya que hacen uso de IoT.

Esta línea de investigación propone:

- Realizar un estudio profundo sobre los riesgos de seguridad que enfrentan los sistemas IoT.
- Realizar un estudio exhaustivo de Android *Things* incluyendo su arquitectura, SO, actualizaciones, etc.
- Integración de aplicaciones basadas en Android *Mobile* y Android *Things*.
- Determinar problemas de seguridad de estas tecnologías.

2.1 Seguridad en IoT

Los principales objetivos de seguridad en IoT son garantizar mecanismos de autenticación de identidad adecuados y proporcionar confidencialidad sobre los datos. Un modelo [15] para desarrollar mecanismos de seguridad en IoT se basa en tres áreas: (i) Confidencialidad de Datos (se utilizan mecanismos de cifrado de datos); (ii) Integridad de Datos (mecanismo cyclic redundancy check. Para evitar el acceso a datos sensibles [7]); disponibilidad de datos (métodos de copia de seguridad de redundancia y conmutación por error. Permiten acceso a sus recursos a quien corresponda en condiciones normales y adversas).

2.2 Android Things

La plataforma Android *Things* es un extensión de la plataforma Android *Mobile* por lo que tiene grandes similitudes en los componentes como por ejemplo: Android SDK, Android Studio, Play Services, FireBase, Google Cloud IoT Core favoreciendo a los desarrolladores de estas tecnologías su flexible y intuitiva convergencia. Se introducen, a continuación, los componentes principales de Android *Things*.

2.2.1 Arquitectura

La arquitectura de Android *Mobile* tradicional se muestra en la Figura 1. Donde se puede observar los núcleos y bibliotecas que son principalmente los encargados de habilitar el soporte del controlador de hardware.

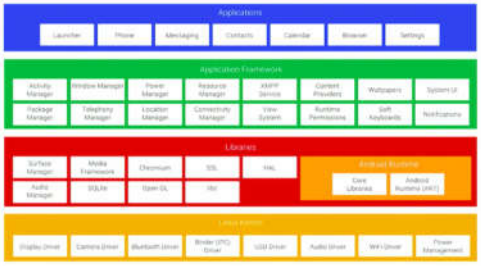

Figura 1: Arquitectura de Android Mobile

Los frameworks de aplicaciones ofrecen un conjunto de APIs con finalidad de ser utilizadas por las mismas. Además, es importante mencionar que las aplicaciones proveen un uso orientado al usuario general como por ejemplo las aplicaciones de mensajería.

Por otro lado, en Android *Things* se eliminan las características mencionadas previamente, como por ejemplo algunas APIs y aplicaciones que están normalmente para el uso cotidiano en Android como las aplicaciones de mensajería. Las pantallas opciones de un dispositivo han sido modificadas en sus comportamientos, como por ejemplo notificaciones, interfaz de usuario; en Android *Things* han sido eliminadas. Por otro lado, cuando el desarrollador trabaja utilizando esta plataforma obtienen la biblioteca de *Things* como soporte para el desarrollo. Esto deja en evidencia que la gestión de dispositivos así como la periferia de entrada/salida esta incorporada en Android *Things*. La Figura 2 muestra la arquitectura de Android *Things* que utiliza un sistema de módulo o arquitectura de SOM.

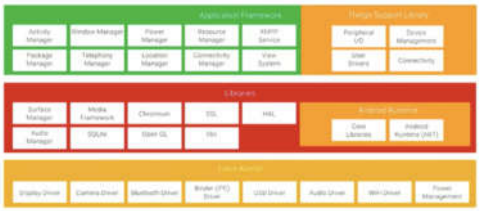

Figura 2: Arquitectura Android Things.

2.2.2 Sistema Operativo

El software que se ejecuta en el dispositivo con Android *Things*, permite construir aplicaciones que utilizan el marco proporcionado por Android *Mobile,* kit de desarrollo de software (SDK) y servicios de Google Play [16]. Esto incluye la misma interfaz de usuario, tookit, soporte multimedia y APIs de conectividad utilizadas por los desarrolladores de *Mobile*. Las aplicaciones se integran fácilmente con los servicios populares de Google, como *Firebase* [17], *TensorFlow* [18] y *Google Cloud Plataform* [19] utilizando la diversidad de bibliotecas de Android *Mobile*.

El desarrollo de Android *Things* utiliza el mismo lenguaje y herramientas que se utiliza para desarrollar Android Mobile. Sin embargo, se ha ajustado la plataforma para reducir los tiempos de arranques como así también reducir el consumo de memoria incluyendo una variantes de servicios de Google Play optimizada específicamente para IoT. Además, se ha agregado nuevas APIs a fin de integrarse adecuadamente con el hardware personalizado; interfaces periféricas y administración de dispositivos.

Por otro lado, Android *Things* no dispone de aplicaciones de usuario como un navegador o indicador. Esto significa que está diseñado para comenzar directamente con las aplicaciones que se han creado para el dispositivo.

2.2.3 Actualizaciones

Google proporciona actualizaciones y parches de seguridad para el sistema operativo central a fin de que el desarrollador se pueda enfocar específicamente en la construcción de la aplicación. Esto permite mantener protegidos a los usuarios en todo momento.

Por otro lado, las imágenes del sistema están firmadas por Google y verificadas para la integridad en el dispositivo lo que evita una actualización corrupta o alterada. En caso de producirse un error en una actualización, el sistema iniciará en un estado conocido previo donde se encuentre estable.

Las actualizaciones se envían por Internet desde la consola Android *Things* utilizando la misma infraestructura segura que se usa para actualizar los dispositivos móviles en la actualidad. Además, previene las actualizaciones automáticamente cuando los parches de seguridad están disponibles para la plataforma.

Las aplicaciones en el dispositivo se administran exclusivamente a través de la consola *Things* e incluye cada actualización, por lo que Android *Things* no incorpora Google Play Store ya que las aplicaciones instalas por el usuario no son soportadas.

Android *Things Console* [20] proporciona herramientas para instalar y actualizar la imagen del sistema en dispositivos de hardware compatibles. Permitiendo enviar actualizaciones a los usuarios así como probar las implementaciones en su propio hardware. La utilización de la consola permite: (i) descargar e instalar la última imagen del sistema Android *Things*; (ii) Crear imágenes de fábrica que contengan aplicaciones OEM junto con la imagen del sistema; (iii) Lanzar las actualizaciones por aire (OTA), incluidas las aplicaciones OEM y la imagen del sistema, a los dispositivos.

2.3 Integración de Android *Things*

Los dispositivos IoT que son desarrollados utilizando Android *Things* cuentan con una placa base de soporte, como por ejemplo el NXP i.MX7D o Raspberry Pi 3 [22]. Para la utilización de estas placas es necesario descargar a la memoria flash o SD Android *Things*. Esta acción permite conectarse a la red Wifi o mediante USB a una computadora. Estas placas posibilitan incorporar hardware adicional conectando a los distintos periféricos accediendo a los protocolos o, a una biblioteca estándar como por ejemplo GPS. Haciendo uso del IDE

Android Studio se inicia la creación del dispositivo IoT.

3. RESULTADOS OBTENIDOS / ESPERADOS

Este trabajo de investigación permitió obtener diferentes resultados que serán utilizados para poder transformar aplicaciones de Android *Mobile* a aplicaciones de Android *Things* confiables e iniciar una metodología o herramienta que automaticen este proceso. Se describen los principales resultados.

Se determinó que Android *Things*: i) permite transformar aplicaciones basadas en Android de una manera transparente y confiable; ii) permite unificar velocidades de procesamiento, minimizar el uso de memoria esto se debe a que Android *Things* ejecuta una única aplicación; iii) en la arquitectura se elimina la capa de aplicación y modifica las APIs, en particular la de la pantalla y la interfaz gráfica; iv) incorpora una consola de actualización gestionada por Google; v) los dispositivos IoT son soportados por una placa base con periféricos de entrada/salida que permiten adaptar hardware adicional conectándose a través de protocolos de comunicación o utilizando la biblioteca estándar.

4. FORMACIÓN DE RECURSOS HUMANOS

Las investigaciones realizadas así como los resultados obtenidos en este trabajo contribuyen al desarrollo de tesis de posgrado, ya sea de doctorado o maestrías en Ingeniería de Software y desarrollo de trabajos finales de las carreras Licenciatura en Ciencias de la Computación, Ingeniería en Informática y Ingeniería en Computación de la Universidad Nacional de San Luis, en el marco de los proyectos de investigación.

5. BIBLIOGRAFÍA

[1] Burnette, E. (2015). *Hello, Android: introducing Google's mobile development platform*. Pragmatic Bookshelf.

[2] Tomás Gironés, J. (2016). *El gran libro de Android*. 4ª. Edición. Alfaomega.

[3] Bustos, M. A., Perez, N. B., & Berón, M. (2015, May). *Plataformas para el desarrollo de aplicaciones móviles. In XVII Workshop de Investigadores en Ciencias de la Computación* (Salta, 2015).

[4] Sitio oficial de Android: https://www.android.com/

[5] Kurniawan, B. (2015). *Java for Android*. Brainy Software Inc.

[6] Zambrano, G. R. (2016). Análisis de Comparación de Android y GNU/Linux/Comparison Analysis Android and GNU/Linux. *International Journal of Innovation and Applied Studies*, *18*(4), 1039.

[7] Londoño, S., Urcuqui, C. C., Cadavid, A. N., Amaya, M. F., & Gómez, J. (2015). SafeCandy: System for security, analysis and validation in Android. *Sistemas & Telemática*, *13*(35), 89-102.

[8] Sultana, S., Enayet, A., & Mouri, I. J. (2015). A Smart, Location Based Time and Attendance Tracking System Using Android Application. *International Journal of Computer Science, Engineering and Information Technology (IJCSEIT)*, *5*(1), 1-5.

[9] Elenkov, N. (2014). *Android security internals: An indepth guide to Android's security architecture*. No Starch Press.

[10] Sitio oficial Android Things: https://developer.android.com/things/index.html

[11] Hahm, O., Baccelli, E., Petersen, H., & Tsiftes, N. (2016). Operating systems for low-end devices in the internet of things: a survey. *IEEE Internet of Things Journal*, *3*(5), 720-734.

[12] Wortmann, F., & Flüchter, K. (2015). Internet of things. Business & Information Systems Engineering, 57(3), 221-224.

[13] DiMarzio, J. F. (2015). Setting Up Android Studio. In *Android Studio Game Development* (pp. 1-8). Apress, Berkeley, CA.

[14] Sitio oficial Android Studio: https://developer.android.com/studio/index.html.

[15] PEREZ, Norma Beatriz, et al. Análisis sistematico de la seguridad en internet of things. En XX Workshop de Investigadores en Ciencias de la Computación (WICC 2018, Universidad Nacional del Nordeste). 2018.

[16] Viennot, N., Garcia, E., & Nieh, J. (2014, June). A measurement study of google play. In *ACM SIGMETRICS Performance Evaluation Review* (Vol. 42, No. 1, pp. 221-233). ACM.

[17] Sitio oficial Firebase: https://firebase.google.com/

[18] Sitio oficial TensorFlow: https://www.tensorflow.org/

[19] Sitio oficial Google Cloud *Plataform*: https://cloud.google.com/

[20] Sitio oficial de desarrollo Android Things: https://developer.android.com/things/console/index.html

[21] Pi, R. (2015). Raspberry Pi Model B.